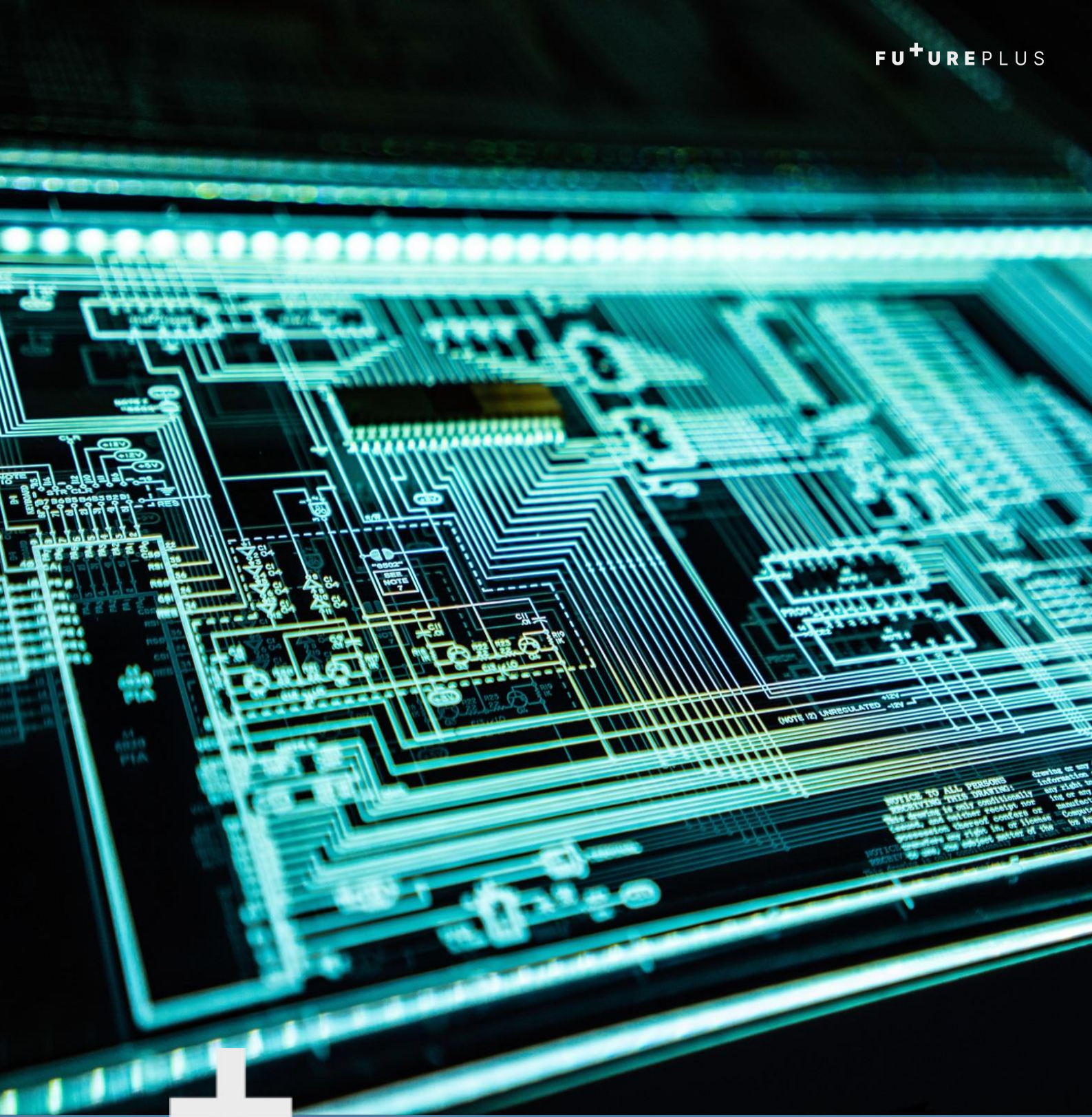
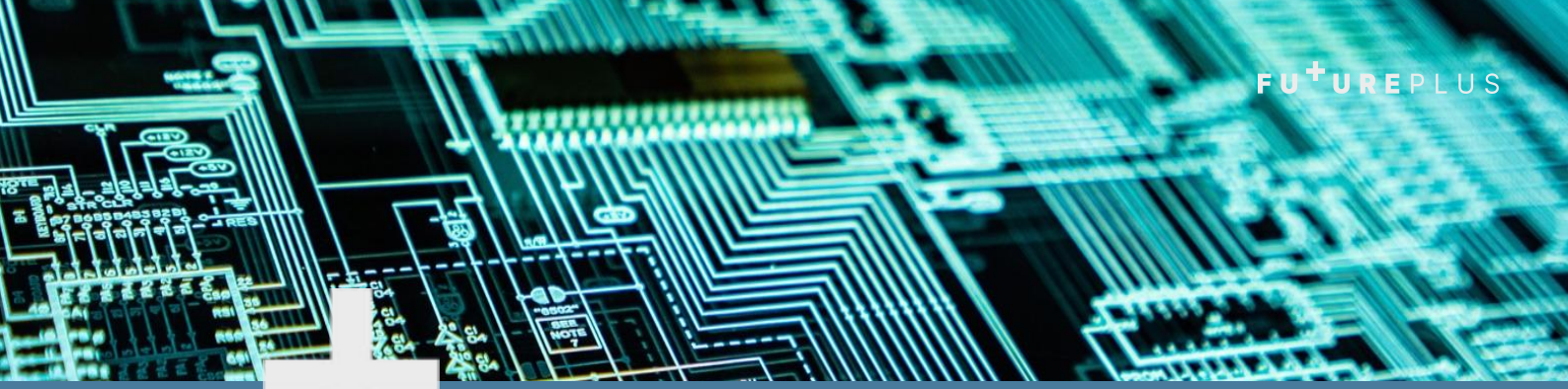
FUTUREPLUS



IT SECURITY

A FUTUREPLUS GUIDE



INTRODUCTION

Customers, employees, and current or potential business partners, of any company, have an expectation that their sensitive information will be respected and given adequate and appropriate protection.

These stakeholders want assurance that their information, systems, and networks are not put “at risk” when they connect to your business. Some of the key reasons for protection include, but are not limited to:

- **Confidentiality** (to ensure that only those who need access to information in order to do their jobs actually have access).
- **Integrity** (to ensure that the information has not been tampered with or deleted by those who should not have had access to it).
- **Availability** (to ensure that the information is available when it is needed by those who conduct the company’s business).

In current times, it is unthinkable to operate a computer without security protection. We hope this guide helps you in understanding what you need to implement in order to protect your information, systems and networks.

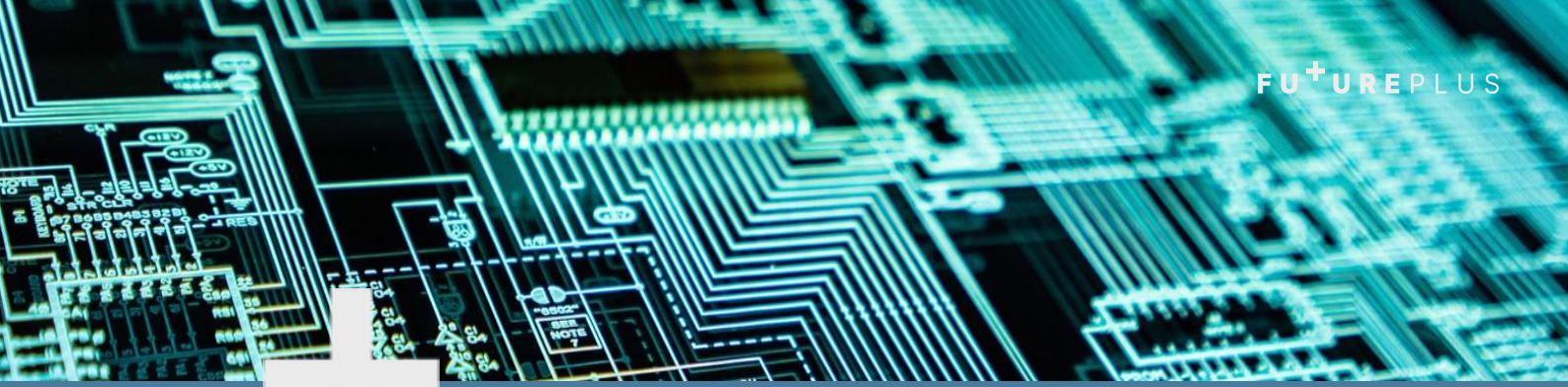
PROTECTION

Protect information, systems, and networks from damage by viruses, spyware, and other malicious code.

Install, use, and keep regularly updated **anti-virus** and **anti-spyware software** on every computer used in your business.

You should be able to set the antivirus software to **automatically** check for updates, this is usually done at night time. Ensure that when you schedule these checks, it is the only activity taking place at any given time.

It is a good idea to obtain copies of your business antivirus software for employees’ **home computers**. Most people do some business work at home, so it is important to protect their home systems, too.



INTERNET CONNECTION SECURITY

Most businesses have broadband access to the Internet. It is important to keep in mind that this type of Internet access is always “on.” Therefore, your computer - or any network your computer is attached to - is exposed to threats from the Internet 24/7.

For broadband Internet access, it is critical to install and keep an operational **hardware firewall** between your internal network and the Internet. This may be a function of a wireless access point/router, or may be a function of a router provided by the Internet Service Provider (ISP).

There are many hardware vendors that provide firewall wireless access points/routers, firewall routers, and firewalls.

If your employees work from home at any point, you should ensure that all employees’ home systems are protected by a hardware firewall between their system(s) and the Internet.

For these devices, **change the administrative password** upon installation and regularly going forward. It is a good idea to change the administrator’s name as well. The default values are easily guessed, and, if not changed, may allow hackers to control your device to monitor or record your communications (and data) to/from the Internet.

SOFTWARE FIREWALLS

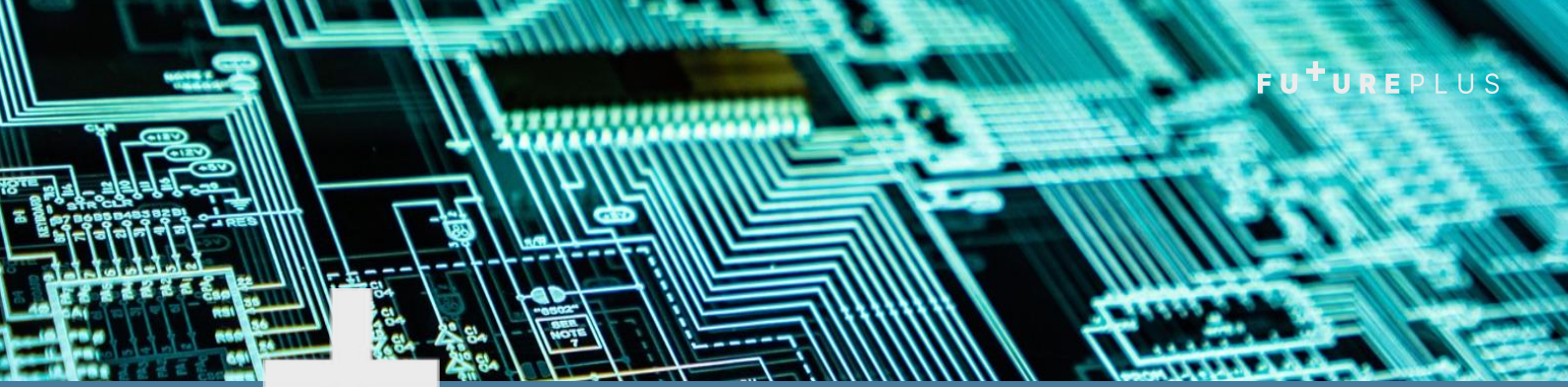
Install, use and activate updated software firewalls on all your business systems.

If you use a Microsoft Windows operating system, it will most likely have a firewall included. You have to ensure that the firewall is **operating**.

When using other commercial operating systems, ensure that you **fully review operations manuals** to determine if your system has a firewall included and how it is enabled.

If employees work from home at any point, you should ensure that their home systems have firewalls installed and operational on them.

It is necessary to have **software firewalls** on each computer even if you have a hardware firewall protecting your network. If your hardware firewall is compromised by a hacker or by malicious code of some kind, software firewalls will help prevent unlimited access to your computers and the information stored on them.



PATCHES

All operating system vendors provide patches and updates to their products to correct security problems and to improve functionality. Ensure that you continue to install the **latest updates**.

BACKUPS & COPIES

It is wise to backup and create copies of your data due to the risk of hard disks failing, computers 'dying', mistakes by employees, and infections by malicious programmes. Data includes (but is not limited to):

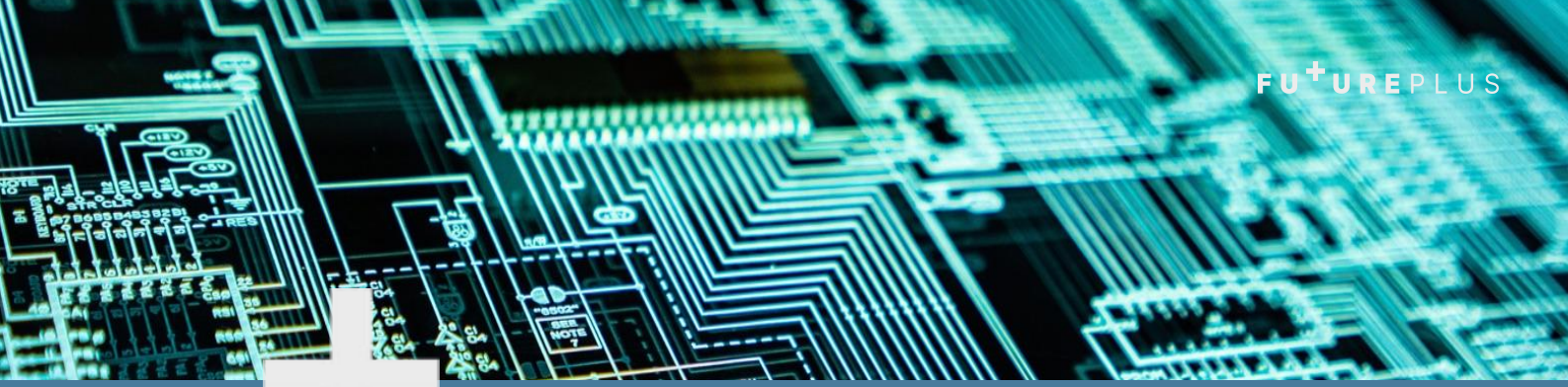
- Word processing documents
- Electronic spreadsheets
- Databases
- Financial files
- Human resources files
- Accounts receivable/payable files
- And other information used in or generated by your business

Remember to periodically **test the backed up data** to ensure it is usable and is being backed up correctly. It is also wise to store backups away from the office location in a protected place.

PASSWORD MANAGEMENT

Set up a **separate account** for each individual and require that strong passwords are used for each account. Strong passwords consist of a **random sequence of letters, numbers**, and **special characters** – and are at least 8 characters long:

- Use strong and unique passwords for all websites and applications
- Reset passwords at regular intervals (we suggest every 3 months)
- Configure two-factor authentication for all accounts
- Store all enterprise passwords in one place and enforce secure password policies within the business environment
- Periodically review violations and take necessary actions



ENCRYPTION

It is important to use **strong encryption** so that data that is transmitted between your computers and wireless access points cannot be easily intercepted and read by electronic eavesdroppers.

Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing it without permission. Encryption is often applied in two different forms:

- **Symmetric key** – or secret key, uses one key to both encode and decode the information. This is best used for one-to-one sharing and smaller data sets.

- **Asymmetric key** – or public key cryptography, uses two linked keys – one private and one public. The encryption key is public and can be used by anyone to encrypt. The opposite key is kept private and used to decrypt.

MALWARE PREVENTION

Malicious programs can be delivered physically to a system through a USB drive or other means, or via the Internet through drive-by downloads, which automatically download malicious programs to users' systems.

Malicious websites and phishing, and scam emails disguised as legitimate messages that contain malicious links or attachments, are two common delivery methods. Keep in mind that there are a lot of more sophisticated malware attacks than these.

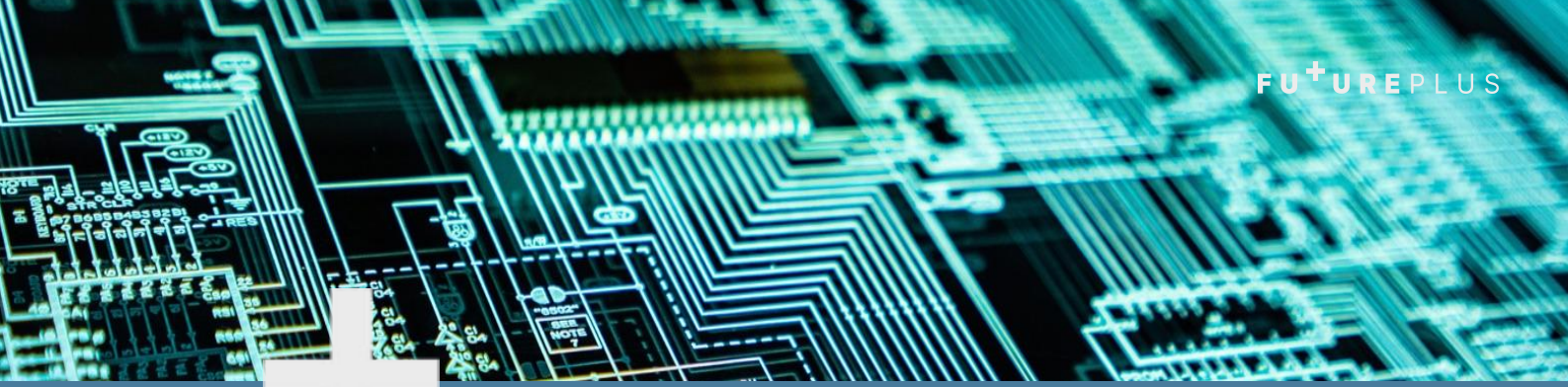
To minimise the risk of any malware, your organisation should adopt at least one of the following approaches:

- Keep anti-malware software **up to date**, with signature files updated at least daily.

- Configure software to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.

- Ensure software scans web pages automatically when they are accessed through a **web browser.**

- Ensure software **prevents** connections to malicious websites.



ID MANAGEMENT

Identity management systems add an additional layer of protection to your business by ensuring user access policies and rules are applied consistently across your organisation. This includes the identification, authentication and authorisation of a person, or persons, to have access to applications, systems or networks. This is done by associating user rights and restrictions with established identities.

NETWORK CONTROLS

Network Security Controls are used to ensure the confidentiality, integrity, and availability of the network services you use for your business. These security controls are either **technical** or **administrative** safeguards, implemented to minimise the security risk. To reduce the risk of a network being compromised, adequate network security requires implementing a proper combination of **network security controls.**

Controlling access to your systems and networks also involves being fully aware of anyone who has access to the systems or networks. This includes, for example, **cleaning staff** who come into office spaces at night, security personal, or maintenance teams. Controlling access also includes being careful about having computer or network repair personnel working unsupervised on systems or devices.

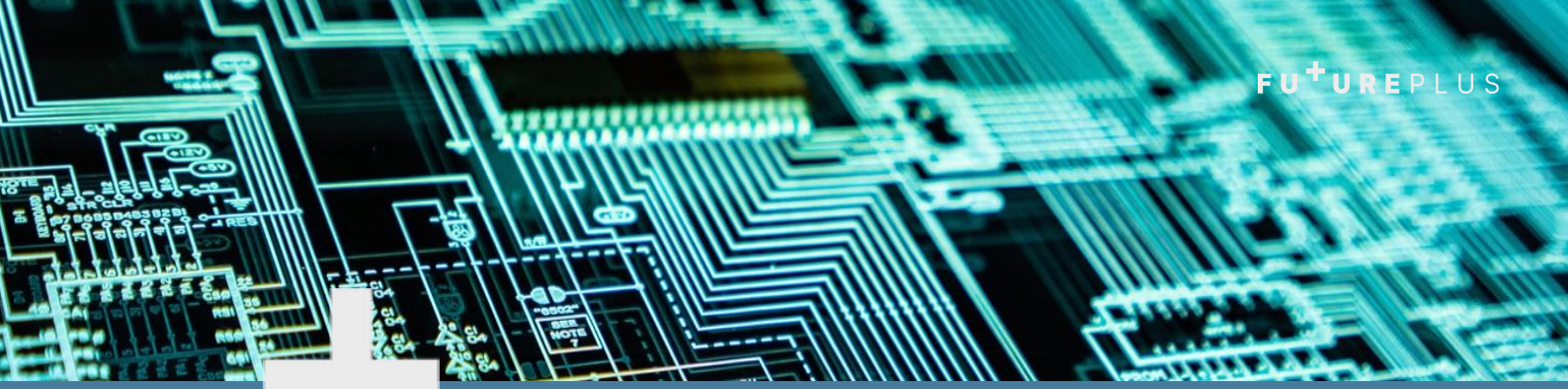
INFORMATION SECURITY CLASSIFICATION

Information Security Classification is the application of a **minimum set of security measures** associated with a 'level' of data. These security measures might change, depending on the information lifecycle stage. It is important to understand that security classification is determined by the level of risk in case of loss or unauthorised access, and **not** by the type of information. It is usually the responsibility of the data owner to classify the data.

Some of the **consequences** of not classifying information correctly include:

- Applying too high a marking can inhibit business operations, such as collaboration, and lead to unnecessary and expensive protective controls being applied.

- Applying too low a marking may result in inappropriate controls, and may put sensitive assets at greater risk of compromise.



SECURITY INCIDENT MANAGEMENT

Security Incident Management is the monitoring and detection of (breaches of) security events that may take place on computers or computer networks.

It is a process that consists of:

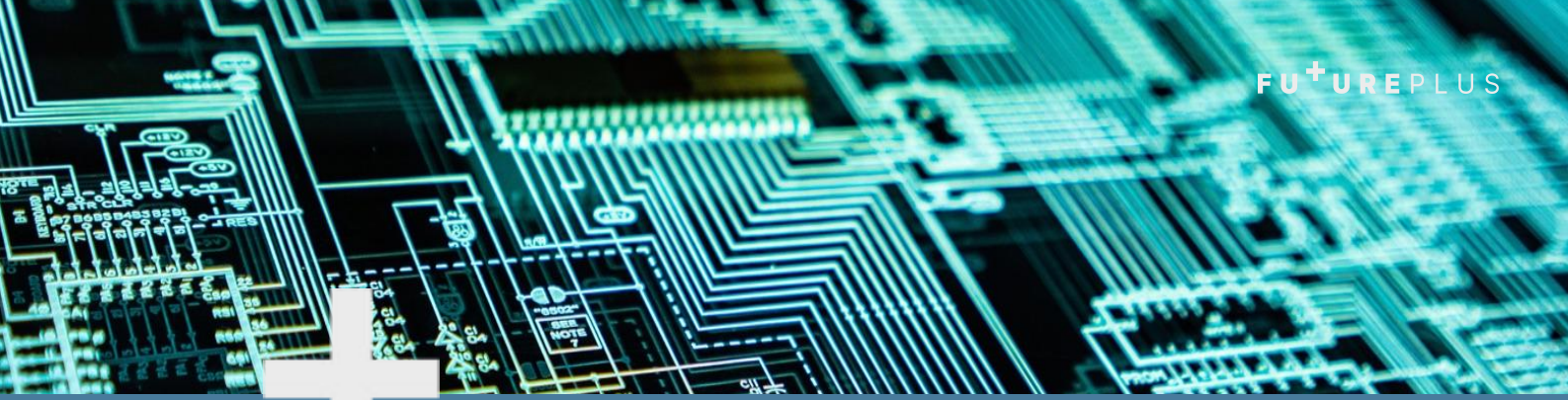
- **preparation**
- **detection**
- **incident containment**
- **mitigation**
- **recovery**

The final phase consists of drawing lessons from the incident that occurred, in order to improve the process and prepare for future incidents. During this cycle, communication with both internal and external stakeholders is essential.

If your company does not have the relevant in-house expertise or skills, you may need to call upon third-party experts to contain an incident if and when it occurs, and/or to carry out forensic investigations.

The following elements should be included in a cyber security incident response plan:

- Think about what needs to be protected – which information, systems, network, products etc.
- Identification and assignment of responsibilities in the event of a breach / incident
- In-house capabilities or contracts with external experts for incident response and/or forensic investigation
- Equipment and technology
- A basic containment strategy
- A communication strategy for both internal and external stakeholders and for authorities such as law enforcement.



CONTINGENCY & DISASTER RECOVERY PLANNING

It is important to have a plan for **restoring business operations** during or after a disaster.

Things to consider:

- Do you have Uninterruptible Power Supplies (UPS) on each of your computers and critical network components? They allow you to work through short power outages and to save your data when the electricity goes off.

- Have you done an inventory of all information used in running your business? Do you know where each type of information is located (on which computer or server).

- Have you prioritised your business information so that you know which type of information is most critical to the operation of your business – and, therefore, which type of information must be restored first in order to run your most critical operations?

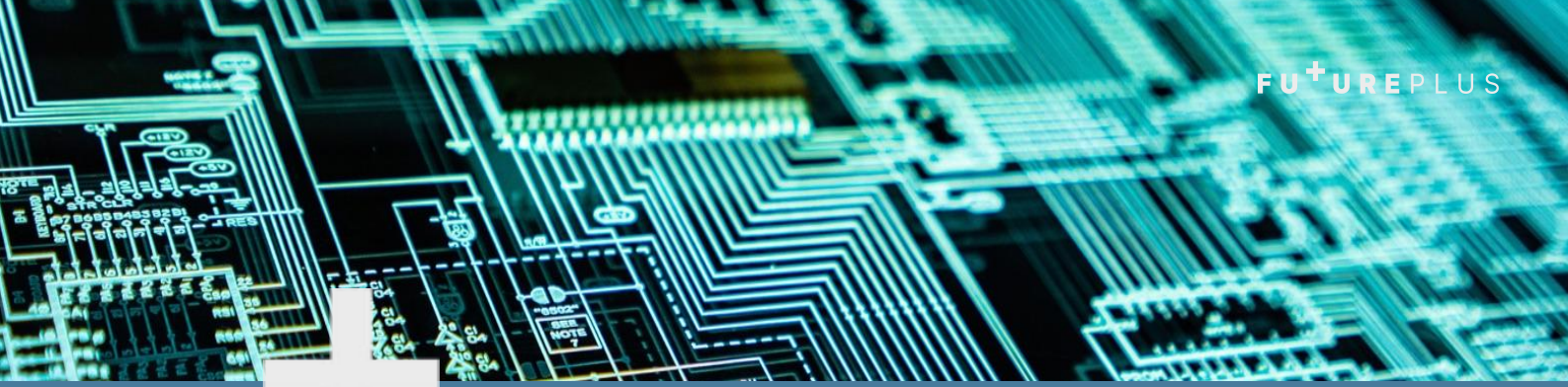
If you have never (or not recently) done a **full inventory** of your important business information, now is the time. For a very small business, this shouldn't take longer than a few hours. For a larger business, this might take from a day to a week or so. (*See Appendix A for a worksheet template for such an inventory*).

After you complete this inventory, ensure that the **information is prioritised** relative to importance for the entire business, not necessarily for a single part of the business. When you have your prioritised information inventory (on an electronic spreadsheet), add three columns to address the kind of protection that each type of information needs.

Some information will need **protection for confidentiality,** some for **integrity**, and some for **availability**. Some might need all three types of protection. *(See Appendix B for a worksheet template for this information).*

This list is useful for when you start to decide how to implement security for your important information and where to spend your resources to protect your important information. Start with the highest priority information, protecting each successive priority level until completed.

In the event of a **security incident** which results in "lost" data because of malicious code, hackers, or employee misconduct, establish procedures to report incidents to employees and/or customers. Ensure you are aware of the regulations and laws requiring specific notifications to affected customers.



INFORMATION HANDLING & DISPOSAL

Data handling is the process of ensuring that any data used by your business is stored, archived, and disposed of in a safe and secure manner. Data handling includes electronic systems, as well as non-electronic systems, such as paper files, journals, notes etc.

Data handling addresses concerns related to **confidentiality**, **security**, **preservation**, and **retention** of data. Proper planning for data handling can also result in efficient and economical storage, retrieval, and disposal of data.

For electronic data, data integrity is a primary concern to ensure that the recorded data is not altered, erased, lost, or accessed by unauthorised users.

Issues that should be considered in ensuring the **integrity of data handled** include:

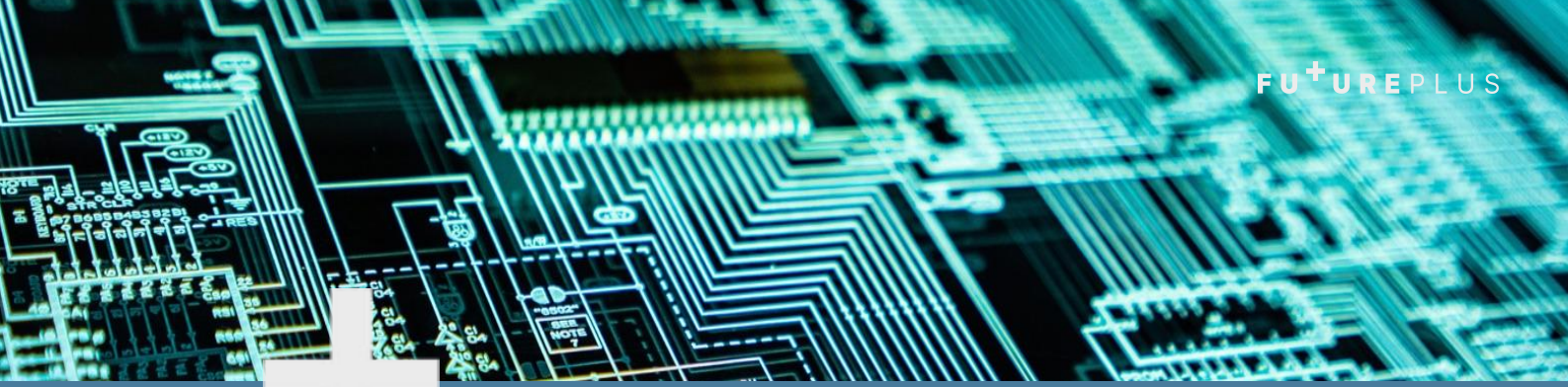
- The type of data being handled;
- The type of media containing data and its storage capacity, handling and storage requirements, reliability, longevity, retrieval effectiveness, and ease of upgrade to newer media;
- Data handling responsibilities/privileges, that is, who can handle which portion of data, at what point during the project, for what purpose, etc; and
- Data handling procedures that describe how long the data should be kept, and when, how, and who should handle data for storage, sharing, archival, retrieval and disposal purposes.

COST-AVOIDANCE CONSIDERATIONS

In information security

It is important to have an idea of how much loss exposure your business may be exposed to if there is a breach in your information security system, such as a malicious program stealing sensitive business information.

There can often be a **real financial and/or reputational cost** associated with not providing adequate protection to sensitive business information.



USE OF CLIENT DATA

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'.

They must make sure that information is:

- Used fairly, lawfully and transparently;
- Used for specified, explicit purposes;
- Used in a way that is adequate, relevant and limited to only what is necessary;
- accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary; and
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

There is stronger legal protection for more sensitive information, such as:

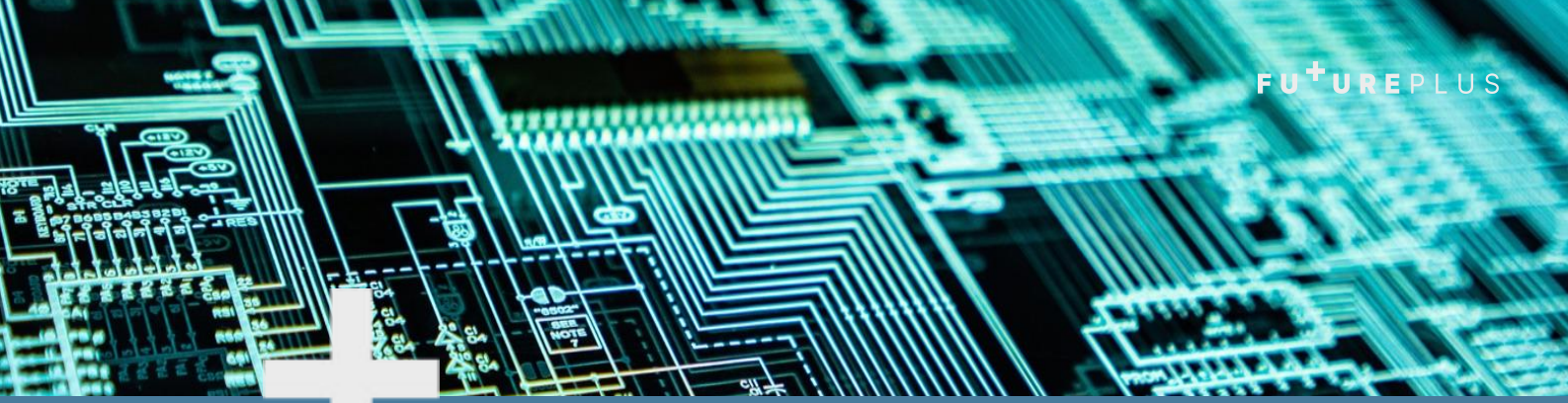
- Race
- Ethnic background
- Political opinions
- Religious beliefs
- Trade union membership
- Genetics
- Biometrics (where used for identification)
- Health
- Sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences. Under the Data Protection Act 2018, consumers have the right to find out what information the government and other organisations store about them. These include the right to:

- Be informed about how their data is being used;
- Access personal data;
- Have incorrect data updated;
- Have data erased;
- Stop or restrict the processing of your data;
- Data portability (allowing you to get and reuse your data for different services); and
- Object to how your data is processed in certain circumstances.

Consumers also have rights when an organisation is using their personal data for:

- Automated decision-making processes (without human involvement); and
- Profiling, for example, to predict their behaviour or interest.



BUSINESS POLICIES

Related to information security and other topics

Policies for information, computer, network, and Internet security, should communicate clearly to employees the **expectations** that the business management has for appropriate use. These policies should identify information and other resources which are important to management and should clearly describe how management expects those resources to be **used and protected** by all employees.

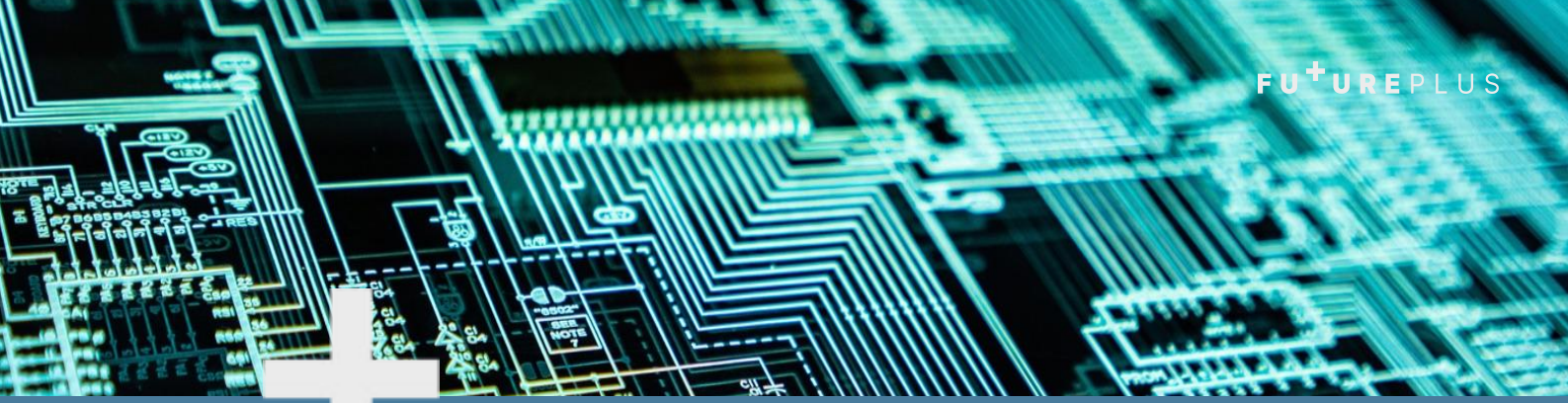
Policies should be **communicated** clearly to each employee and all employees should sign a **statement** agreeing that they have read the policies, that they will follow the policies, and that they understand the possible penalties for violating those policies. This will help management to hold employees **accountable** for violation of business policies.

As noted, there should be penalties for disregarding business policies. And, those penalties should be enforced fairly and consistently for everyone in the business that violates the policies of the business.

NEED MORE HELP?

We offer in-house consultancy services if you need more help with your IT security, and would love to hear from you.

Get in touch at: team@future-plus.co.uk



Appendix A:

Identifying and prioritising your businesses information types.

- Think about the information used in, or by your business, and make a list of all the information types used in your business (define “information type” in any useful way that makes sense to your business).

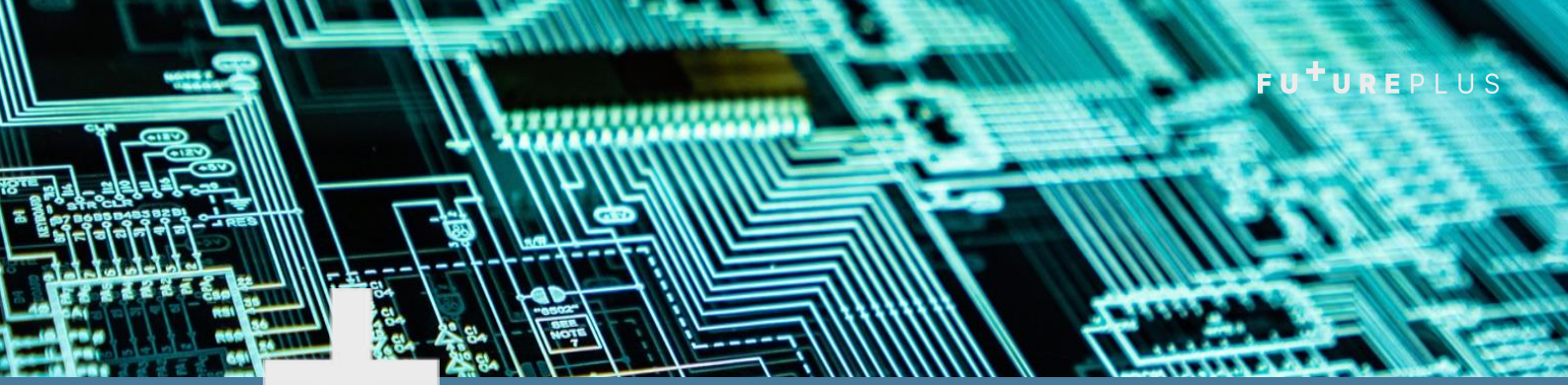
- List and prioritise the most important types of information used in your business and enter them into the table below.

- Identify the system on which each information type is located.

- Finally, create a complete table for all your business information types – in priority order.

Table 1 – Priority information types in my business

PRIORITY	TYPE OF INFORMATION	STORED ON WHICH SYSTEM?
1.		
2.		
3.		



Appendix B:

Identifying the protection needed by your organisation's priority information types.

- Think about the information used in/by your business.
- Enter the highest priority information types in your business into the table below.
- Enter the protection required for each information type in the columns to the right.
- (C – Confidentiality; I – Integrity; A - Availability) <"Y"-needed; "N"-not needed>.
- Finally, finish a complete table for all your business information types. (Note: this would usually be done by adding three columns to Table 1).

Table 2 – The protection needed by the highest priority information types in my business

PRIORITY	TYPE OF INFORMATION	C	I	A
1				
2				
3				